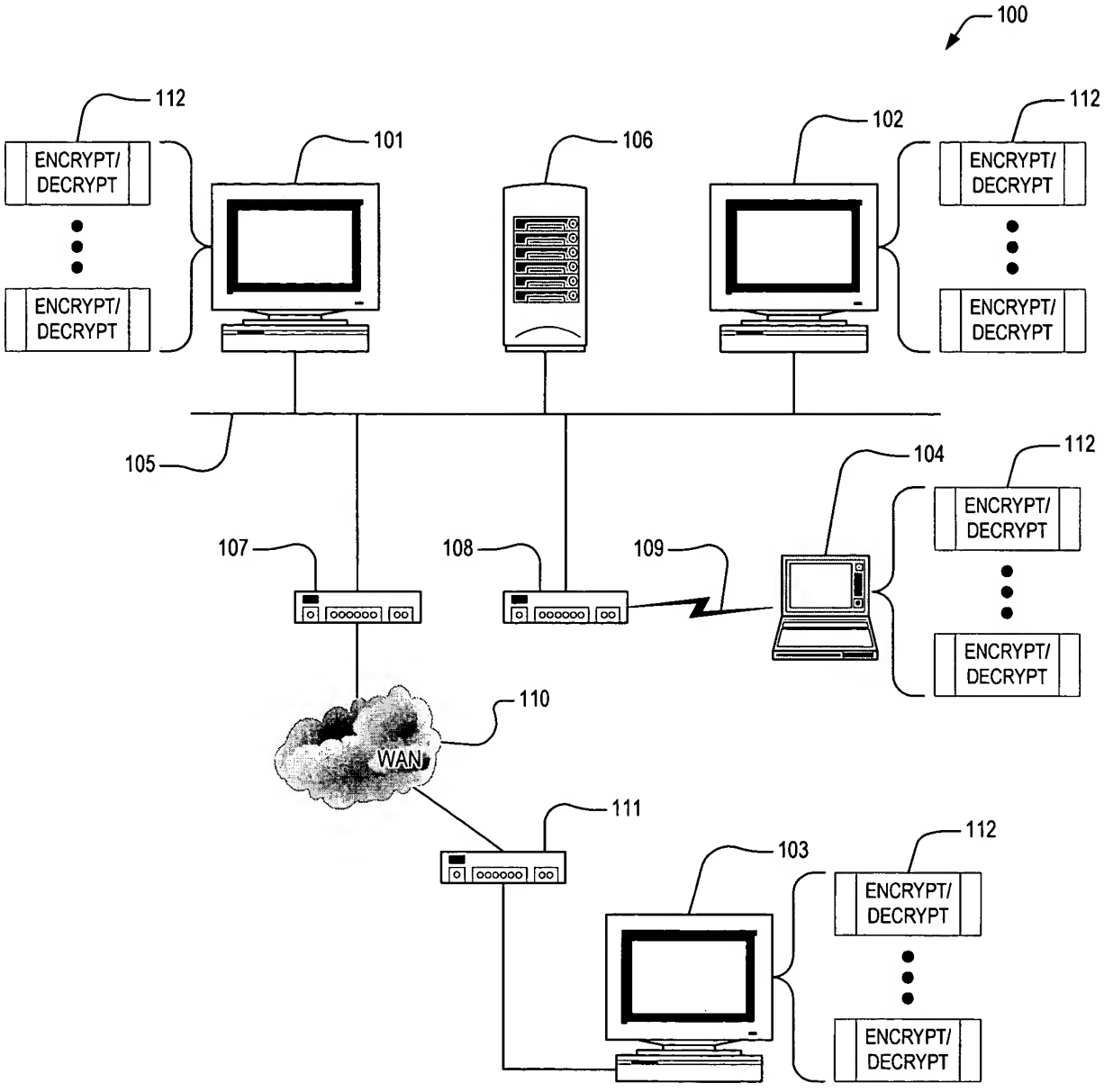
100
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT
101
106
102
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT
105
104
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT
107
108
109
110
WAN
111
103
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT

FIG. 1

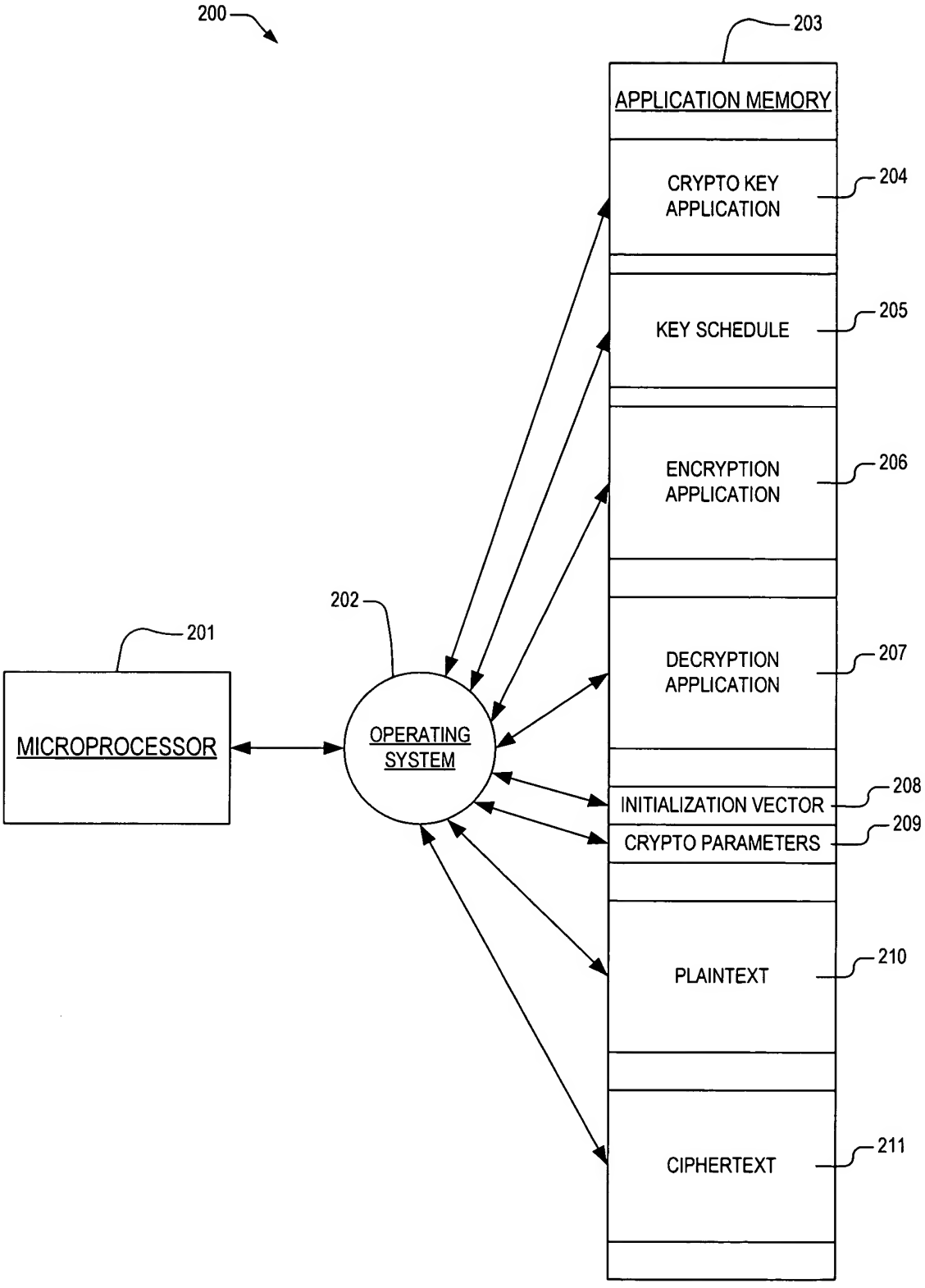
200
203
APPLICATION MEMORY
CRYPTO KEY APPLICATION
204
KEY SCHEDULE
205
ENCRYPTION APPLICATION
206
DECRYPTION APPLICATION
207
INITIALIZATION VECTOR
208
CRYPTO PARAMETERS
209
PLAINTEXT
210
CIPHERTEXT
211
202
OPERATING SYSTEM
201
MICROPROCESSOR

FIG. 2

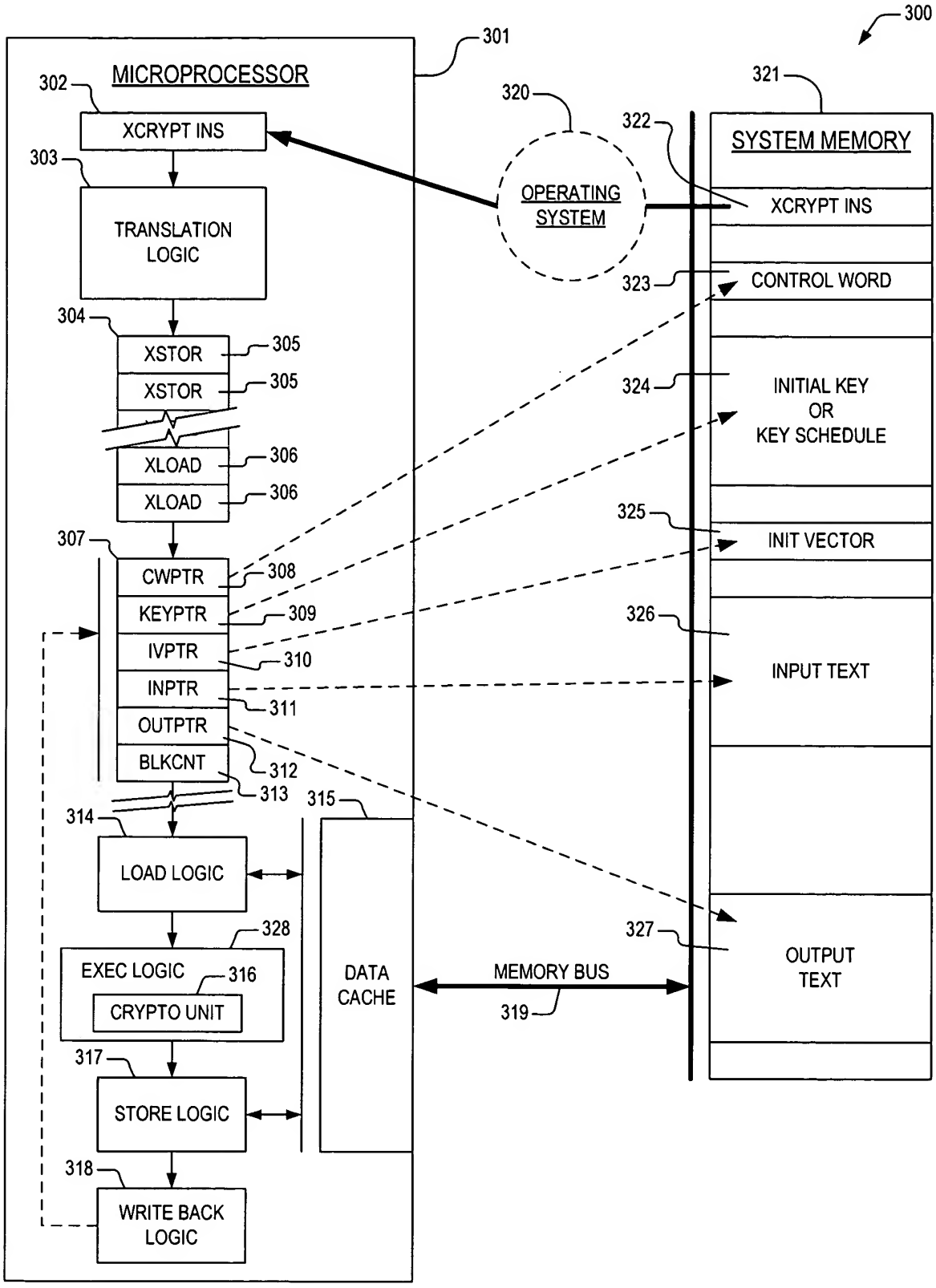
300
301
MICROPROCESSOR
302
XCRYPT INS
303
TRANSLATION LOGIC
304
XSTOR
305
XSTOR
305
XLOAD
306
XLOAD
306
307
CWPTR
308
KEYPTR
309
IVPTR
310
INPTR
311
OUTPTR
312
BLKCNT
313
314
LOAD LOGIC
328
EXEC LOGIC
316
CRYPTO UNIT
317
STORE LOGIC
318
WRITE BACK LOGIC
315
DATA CACHE
MEMORY BUS
319
320
OPERATING SYSTEM
321
SYSTEM MEMORY
322
XCRYPT INS
323
CONTROL WORD
324
INITIAL KEY OR KEY SCHEDULE
325
INIT VECTOR
326
INPUT TEXT
327
OUTPUT TEXT

FIG. 3

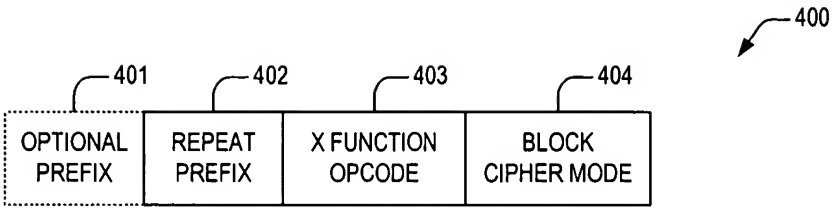

FIG. 4

500

BCM VALUE	MODE
0xC8	ELECTRONIC CODE BOOK (ECB)
0xD0	CIPHER BLOCK CHAINING (CBC)
0xE0	CIPHER FEEDBACK (CFB)
0xE8	OUTPUT FEEDBACK (OFB)
ALL OTHER VALUES	RESERVED

FIG. 5

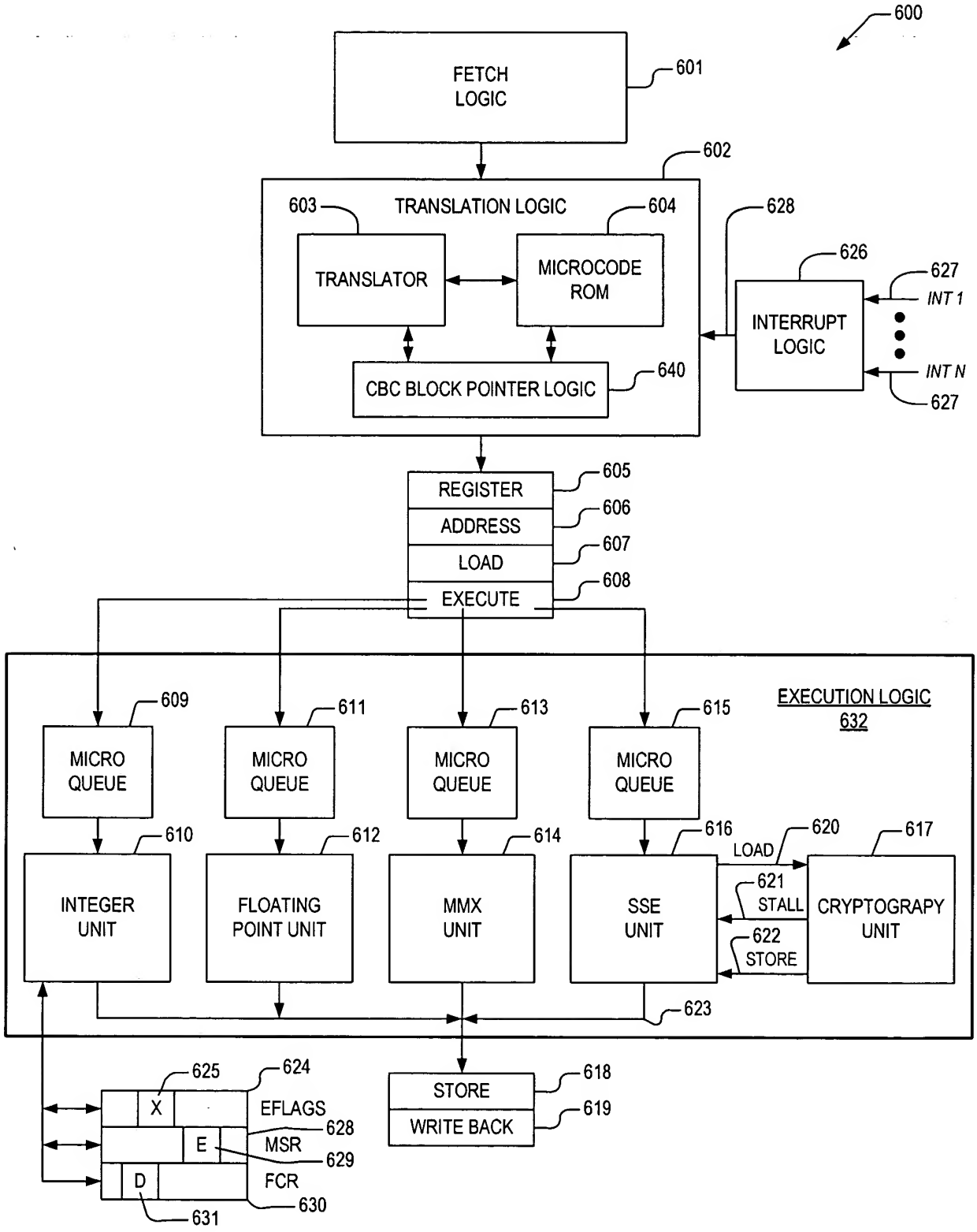
600
FETCH LOGIC
601
602
TRANSLATION LOGIC
603
TRANSLATOR
604
MICROCODE ROM
CBC BLOCK POINTER LOGIC
640
628
626
INTERRUPT LOGIC
627
INT 1
INT N
627
REGISTER
ADDRESS
LOAD
EXECUTE
605
606
607
608
EXECUTION LOGIC
632
MICRO QUEUE
609
MICRO QUEUE
611
MICRO QUEUE
613
MICRO QUEUE
615
INTEGER UNIT
610
FLOATING POINT UNIT
612
MMX UNIT
614
SSE UNIT
616
LOAD
620
621
STALL
622
STORE
CRYPTOGRAPY UNIT
617
623
X
EFLAGS
624
625
E
MSR
628
629
D
FCR
630
631
STORE
618
WRITE BACK
619

FIG. 6

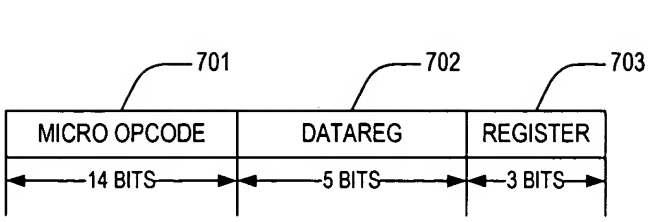

FIG. 7

800

VALUE	OPERATION
000	RESERVED
001	RESERVED
010	LOAD CONTROL WORD (CW) REGISTER
011	RESERVED
100	LOAD INPUT-0 (IN-0) REGISTER AND START CRYPTOGRAPHY UNIT
101	LOAD INPUT-1 (IN-1) REGISTER
110	LOAD CRYPTO KEY-0 REGISTER (LOWER 128 BITS OF KEY)
111	LOAD CRYPTO KEY-1 REGISTER (UPPER 128 BITS OF KEY)

FIG. 8

900

VALUE	OPERATION
000	RESERVED
001	RESERVED
010	RESERVED
011	RESERVED
100	STORE OUTPUT-0 (OUT-0) REGISTER
101	STORE OUTPUT-1 (OUT-1) REGISTER
110	RESERVED
111	RESERVED

FIG. 9

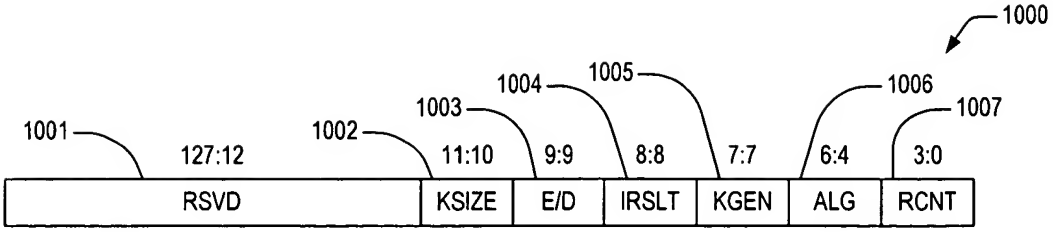
1000
1001
127:12
RSVD
1002
11:10
KSIZE
1003
9:9
E/D
1004
8:8
IRSLT
1005
7:7
KGEN
1006
6:4
ALG
1007
3:0
RCNT

FIG. 10

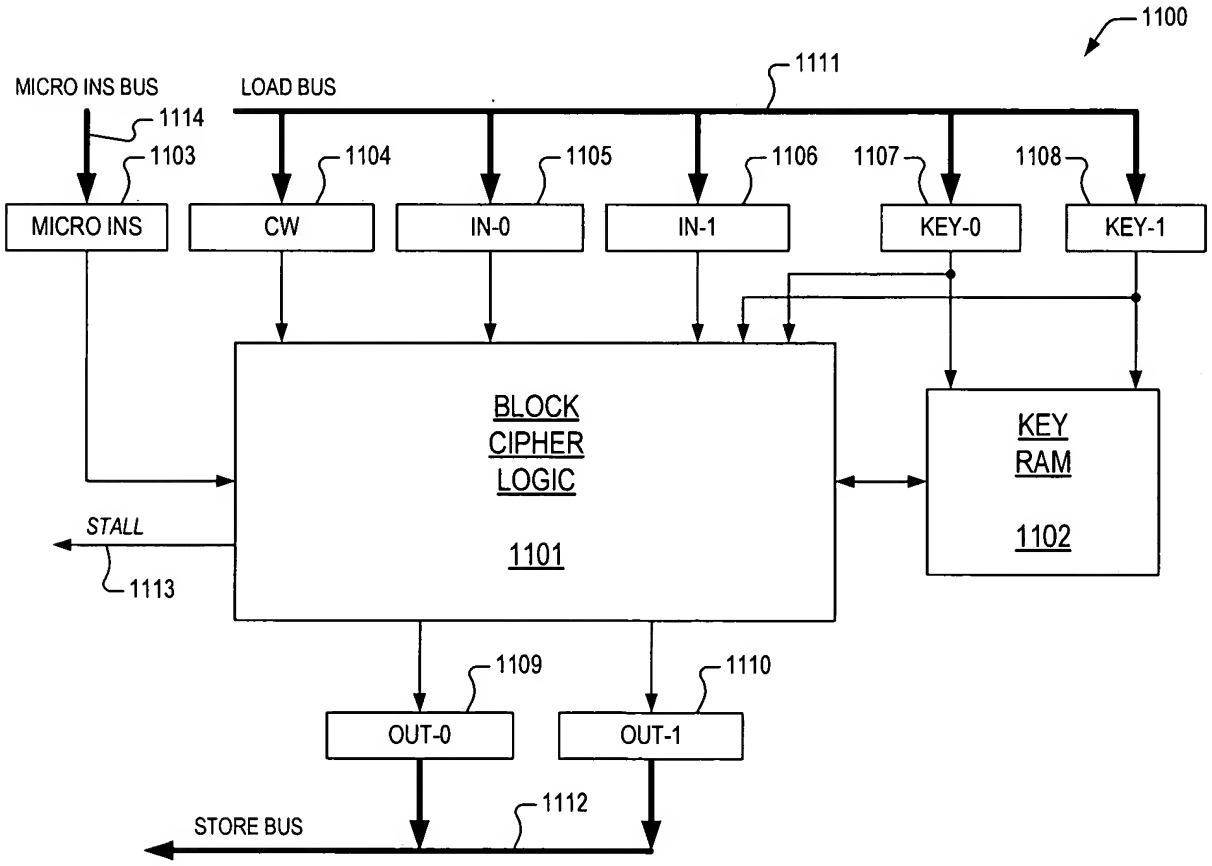
1100
1111
MICRO INS BUS
LOAD BUS
1114
1103
1104
1105
1106
1107
1108
MICRO INS
CW
IN-0
IN-1
KEY-0
KEY-1
BLOCK
CIPHER
LOGIC
1101
KEY
RAM
1102
STALL
1113
1109
1110
OUT-0
OUT-1
1112
STORE BUS

FIG. 11

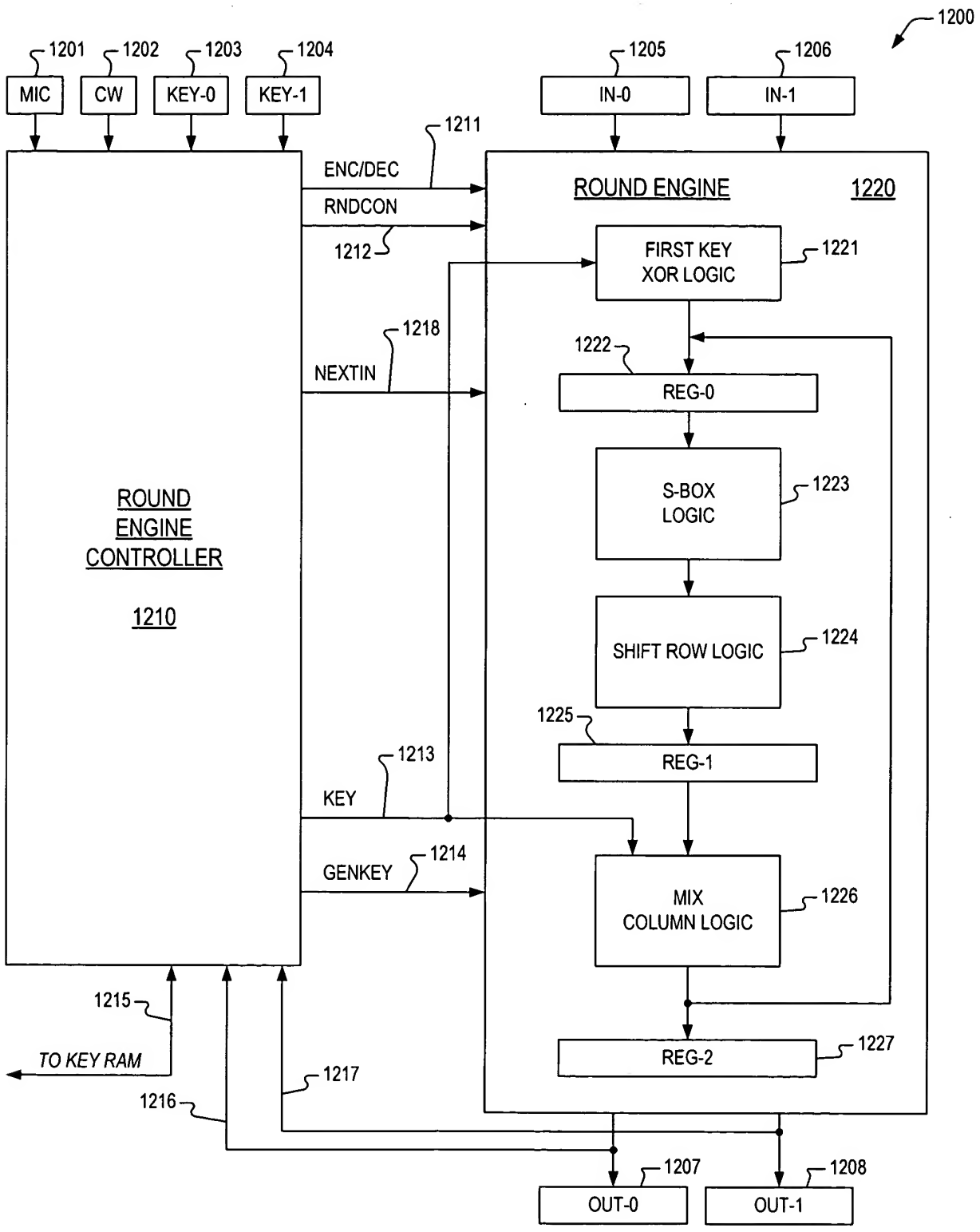
1200
1201
1202
1203
1204
1205
1206
MIC
CW
KEY-0
KEY-1
IN-0
IN-1
1211
ENC/DEC
RNDCON
1212
ROUND ENGINE
1220
FIRST KEY XOR LOGIC
1221
1218
NEXTIN
1222
REG-0
S-BOX LOGIC
1223
ROUND ENGINE CONTROLLER
1210
SHIFT ROW LOGIC
1224
1225
REG-1
1213
KEY
GENKEY
1214
MIX COLUMN LOGIC
1226
1215
TO KEY RAM
REG-2
1227
1217
1216
1207
1208
OUT-0
OUT-1

FIG. 12

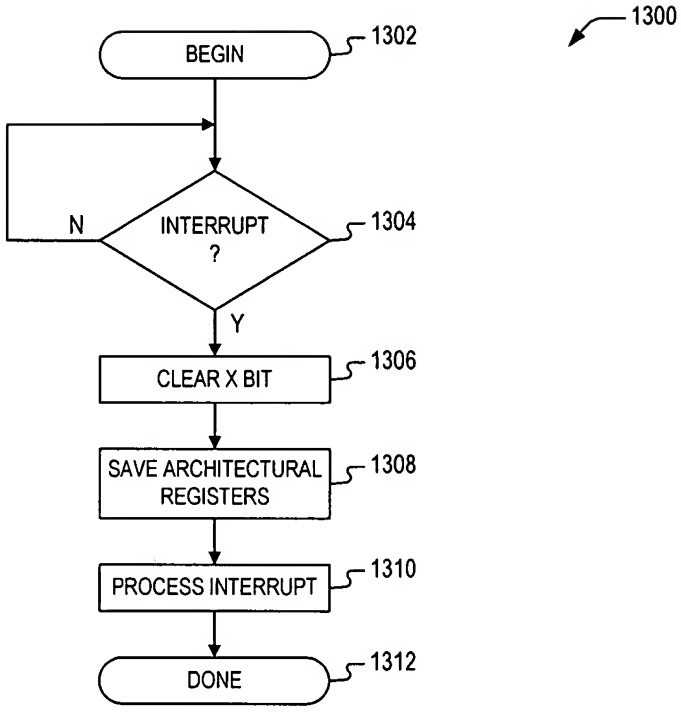
1300
BEGIN
1302
INTERRUPT ?
1304
N
Y
CLEAR X BIT
1306
SAVE ARCHITECTURAL REGISTERS
1308
PROCESS INTERRUPT
1310
DONE
1312

FIG. 13

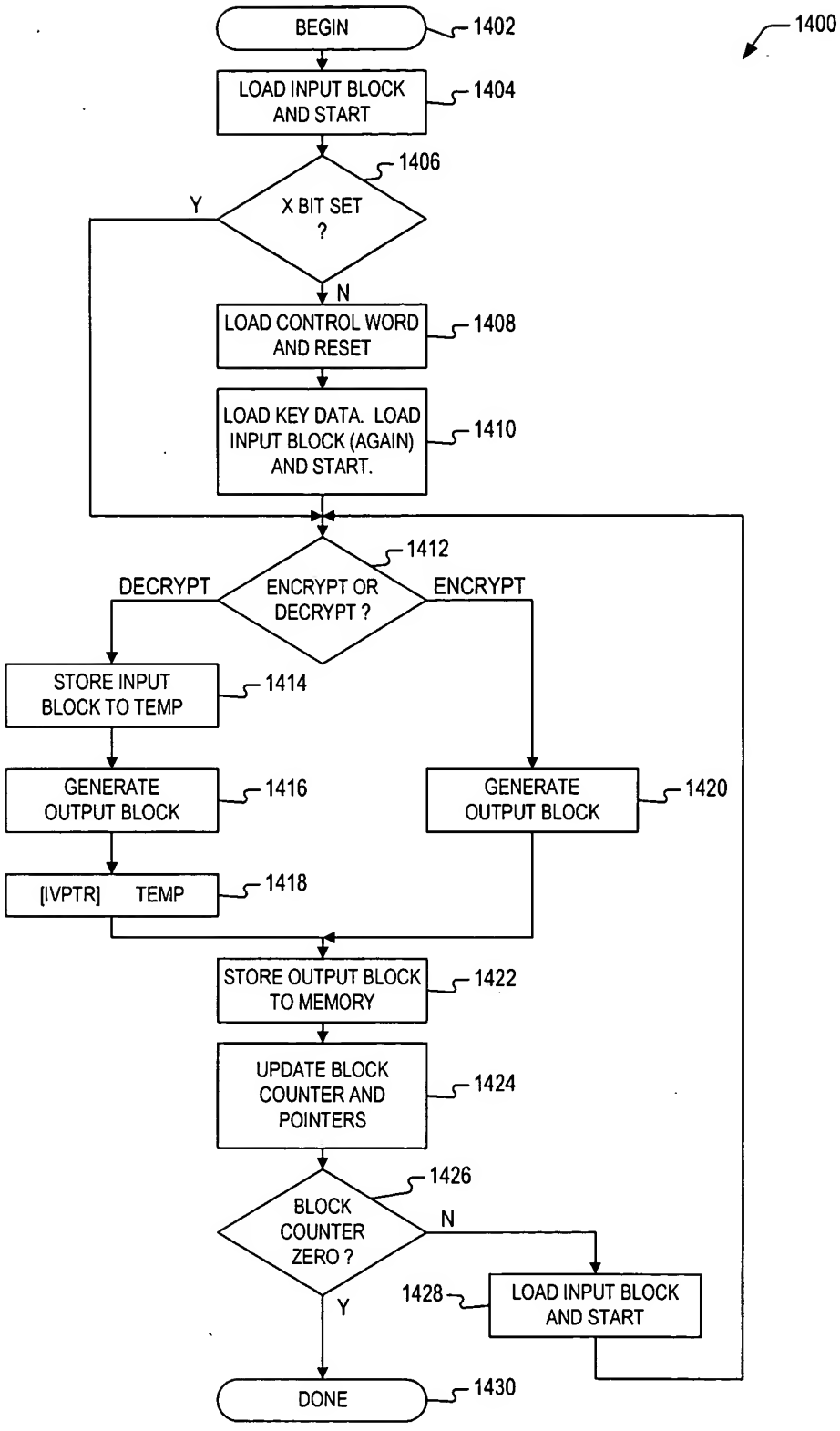
1400
BEGIN
1402
LOAD INPUT BLOCK AND START
1404
1406
X BIT SET ?
Y
N
LOAD CONTROL WORD AND RESET
1408
LOAD KEY DATA. LOAD INPUT BLOCK (AGAIN) AND START.
1410
1412
ENCRYPT OR DECRYPT ?
DECRYPT
ENCRYPT
STORE INPUT BLOCK TO TEMP
1414
GENERATE OUTPUT BLOCK
1416
GENERATE OUTPUT BLOCK
1420
[IVPTR] TEMP
1418
STORE OUTPUT BLOCK TO MEMORY
1422
UPDATE BLOCK COUNTER AND POINTERS
1424
1426
BLOCK COUNTER ZERO ?
N
Y
1428
LOAD INPUT BLOCK AND START
DONE
1430

FIG. 14